IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

DON HAYS, ON BEHALF OF HIMSELF AND ALL OTHERS SIMILARLY SITUATED,	§	
Plaintiff,	§	SA-23-CV-01490-FB
vs.	§	
FROST & SULLIVAN, INC.,	§	
Defendant.	§	

REPORT AND RECOMMENDATION
OF UNITED STATES MAGISTRATE JUDGE

To the Honorable United States District Judge Fred Biery:

This Report and Recommendation concerns Defendant Frost & Sullivan, Inc.'s Rule 12(b)(1) Motion to Dismiss for Lack of Subject Matter Jurisdiction and Rule 12(b)(6) Motion to Dismiss for Failure to State a Claim [#7]. All pretrial matters in this case have been referred to the undersigned for disposition pursuant to Western District of Texas Local Rule CV-72 and Appendix C [#10]. The undersigned has authority to enter this recommendation pursuant to 28 U.S.C. § 636(b)(1)(B). After considering Plaintiff's response to the motion [#15] and Defendant's reply [#16] and for the reasons set forth below, it is recommended that Defendant's motion to dismiss be granted in part as to Plaintiff's breach of fiduciary duty and invasion of privacy claims. In all other respects, the motion should be denied.

I. Background

Plaintiff Don Hays filed his Class Action Complaint, on behalf of himself and all others similarly situated, against Defendant Frost & Sullivan, Inc., alleging Defendant's failure to

protect the highly sensitive data of its current and former employees and clients from a data breach. According to the Complaint, Defendant is a business consulting firm with 1,200 employees in 45 offices across the globe. (Compl. [#1], at ¶ 13.) Defendant has a Privacy Policy in which it outlines its duties to employees and clients regarding their sensitive personal information and describes the company's security policies and procedures protecting data from unauthorized access. (*Id.* at ¶ 19.)

The Complaint alleges that from March 10, 2023, to July 8, 2023, Defendant was the target of a cyberattack and the personal identifiable information ("PII") (names and Social Security numbers) of at least 279 employees and clients was exposed. (*Id.* at ¶¶ 13, 20–23.) According to the Complaint, Defendant waited until September 5, 2023, 59 days after it noticed the data breach, to notify the proposed class members of the breach and the resulting risk of identity theft. (*Id.* at ¶¶ 24–26.) Plaintiff is a former employee of Defendant who alleges his PII was compromised in the data breach and that he was injured as a result of the breach. (*Id.* at ¶¶ 38–40.) Plaintiff claims that he worked for Defendant for approximately 20 years and provided his PII as part of the employer-employee relationship. (*Id.* at ¶ 41.) Plaintiff's Complaint proposes the following class of plaintiffs:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Frost & Sullivan in July 2023, including all those individuals who received notice of the breach.

(*Id.* at ¶ 80.)

Plaintiff's Complaint contains specific allegations regarding the nature of the cyberattack based on several news reports regarding the data breach. According to the Complaint, the stolen data has already been sold "on a hacker forum," because a group known as "KelvinSecurty Team" posted on the forum that it was selling various databases related to Defendant's

employees and customers, including "6,000 customer records and 6,146 records for companies." (*Id.* at ¶ 33.) The Complaint further alleges that "the Akira ransomware gang" has already "dropped over 90 gigabytes of data belonging to [Defendant] on its darknet leak site" and that an additional 90 gigabytes of data "will be available soon" from the breach. (*Id.* at ¶ 35.)

Plaintiff pleads that on information and belief his PII has already been published or will be published imminently by cybercriminals on the dark web, where data obtained through hacking is purchased and sold. (*Id.* at ¶¶ 34, 45.) Plaintiff alleges he has spent and will continue to spend significant uncompensated time and effort monitoring his accounts to protect himself from identity theft by enrolling in credit monitoring service and has suffered from a spike in spam messages and phone calls. (*Id.* at ¶¶ 48–49.) Plaintiff claims he fears for his personal financial security; suffers from anxiety, sleep disruption, stress, fear, and frustration; and worries about what information was exposed in the data breach. (*Id.* at ¶¶ 50–51.) Plaintiff asserts that he has suffered actual injury from the exposure of theft of his PII based on the foregoing, as well as the diminution in the value of his PII (a valuable commodity on the criminal black market) and a substantially increased risk of fraud, misuse, and identity theft. (*Id.* at ¶¶ 52–54, 58.)

Based on these allegations, Plaintiff asserts causes of action for negligence (Count One), negligence *per se* (Count Two), breach of implied contract (Count Three), breach of fiduciary duty (Count Four), invasion of privacy (Count Five), and unjust enrichment (Count Six). (*Id.* at ¶¶ 90–169.) Plaintiff seeks damages both on behalf of himself and the proposed class and injunctive relief as necessary to protect the interests of Plaintiff and the class through this suit. (*Id.* at ¶¶ 36–37.) Defendant has moved to dismiss Plaintiff's Class Action Complaint for lack of subject matter jurisdiction pursuant to Rule 12(b)(1) and failure to state a claim pursuant to Rule 12(b)(6). Defendant argues Plaintiff lacks standing to assert his claims because he has not

suffered a cognizable injury in fact because he does not allege that he has been the victim of identity theft or fraud due to the data breach. Defendant also argues that some of Plaintiff's tort claims fail as a matter of law due to pleading deficiencies or legal defects with the claims. The parties appeared before the undersigned for an initial pretrial conference on April 3, 2024, and the undersigned heard brief argument on the motion. The undersigned has considered the parties' arguments from the conference as well as their written filings, and the motion is ripe for the Court's review.

II. Standing

Defendant first argues Plaintiff lacks standing to bring any of his claims and requests dismissal of his entire Class Action Complaint for lack of subject matter jurisdiction on this basis. The Court should deny Defendant's jurisdictional challenge because Plaintiff has pleaded a cognizable injury in fact for standing purposes to pursue his claims for both damages and injunctive relief.

A. Legal Standards

Motions filed under Rule 12(b)(1) allow a party to challenge the subject-matter jurisdiction of the district court to hear a case. Fed. R. Civ. P. 12(b)(1); *Ramming v. United States*, 281 F.3d 158, 161 (5th Cir. 2001). To survive a Rule 12(b)(1) motion to dismiss, a plaintiff must establish this Court's jurisdiction through sufficient allegations. *See Lujan v. Def. of Wildlife*, 504 U.S. 555, 561 (1992). "A case is properly dismissed for lack of subject matter jurisdiction when the court lacks the statutory or constitutional power to adjudicate the case." *Home Builders Ass'n of Miss., Inc. v. City of Madison, Miss.*, 143 F.3d 1006, 1010 (5th Cir. 1998) (quoting *Nowak v. Ironworkers Local 6 Pension Fund*, 81 F.3d 1182, 1187 (2d Cir. 1996)). "A court may base its disposition of a motion to dismiss for lack of subject matter

jurisdiction on (1) the complaint alone; (2) the complaint supplemented by undisputed facts; or (3) the complaint supplemented by undisputed facts plus the court's resolution of disputed facts." *Montez v. Dep't of Navy*, 392 F.3d 147, 149 (5th Cir. 2004) (quoting *Robinson v. TCI/US W. Commc'ns Inc.*, 117 F.3d 900, 904 (5th Cir. 1997)). The burden of proof rests on the party asserting jurisdiction. *Ramming*, 281 F.3d at 161.

Absent standing, a federal court does not have subject matter jurisdiction to address a plaintiff's claims. *Cobb v. Cent. States*, 461 F.3d 632, 635 (5th Cir. 2006). The doctrine of standing addresses the question of who may properly bring suit in federal court and "is an essential and unchanging part of the case-or-controversy requirement of Article III." *Lujan*, 504 U.S. at 560. Article III standing requires the satisfaction of three elements: (1) a concrete and particularized injury-in-fact, either actual or imminent; (2) a causal connection between the injury and defendant's challenged conduct; and (3) a likelihood that the injury suffered will be redressed by a favorable decision. *Id.* at 560–61. Defendant's motion focuses on the first requirement of standing—that a plaintiff must have suffered a concrete and particularized injury in fact to seek redress in federal court. "In class actions, 'named plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class.'" *Brown v. Protective Life Ins. Co.*, 353 F.3d 405, 407 (5th Cir. 2003) (quoting *Lewis v. Casey*, 518 U.S. 343, 357 (1996)).

B. Analysis

Defendant contends that Plaintiff's Complaint fails to allege a concrete injury because Plaintiff alleges nothing more than a speculative and hypothetical risk of future harm caused by the data breach. More specifically, Defendant argues Plaintiff must allege he has been a victim of actual or attempted identity theft to have standing to pursue his claims.

Plaintiff responds that allegations of identity theft are not required to establish Article III standing. Plaintiff argues he has standing to pursue his tort claims for damages and injunctive relief because publication of his PII on the dark web is itself a violation of his privacy and a concrete injury. Plaintiff further argues that he has suffered the following additional injuries, each sufficient to confer standing: an increased risk of identity theft and fraud; the lost property value of his PII; psychological injuries of anxiety, sleep disruption, stress, fear, and frustration; a spike in scam messages and calls targeting Plaintiff; the expenditure of time spent responding to the data breach and mitigating the possibility of future harm; and the violation of his implied contractual rights regarding the preservation of the confidentiality of his PII. The undersigned agrees with Plaintiff that he has sufficiently pleaded an injury in fact for purposes of establishing his standing under Article III.

The Supreme Court has explained that for an injury to be cognizable for standing purposes, it must be "concrete, particularized, and actual or imminent." *Clapper v. Amnesty Int'l*, 568 U.S. 398, 409 (2013) (internal quotation and citation omitted). The Supreme Court has recognized three kinds of concrete harm: (1) tangible harms, like physical or monetary harms; (2) intangible harms, so long as those injuries bear a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts; and (3) a sufficiently imminent and substantial material risk of future harm when a plaintiff is seeking injunctive relief, not damages. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425, 435–36 (2021). To have standing to pursue damages based on a risk of future harm, in addition to the imminence of the future harm, plaintiffs must also demonstrate a separate concrete harm caused "by their exposure to the risk itself." *Id.* at 438.

An imminent injury is one which is "certainly impending" or for which there is a "substantial risk" that the harm will occur. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 414 n.5). While plaintiffs are not required "to demonstrate that it is literally certain that the harms they identify will come about," a possible future injury—even one with an objectively reasonable likelihood of occurring—is not sufficient to satisfy the concrete-injury requirement. *Clapper*, 568 U.S. at 409–10, 414 n.5 (emphasis omitted).

The Supreme Court most recently addressed these principles in *TransUnion LLC v. Ramirez*. In *TransUnion*, a plaintiff filed a class action on behalf of himself and over 8,000 class members seeking statutory damages for the alleged violation of the Fair Credit Reporting Act. 594 U.S. at 417–18. The lead plaintiff alleged that TransUnion had erroneously placed an alert on his credit report and the reports of numerous other consumers, indicating that he was a potential match to an individual on a list of "specially designated nationals who threaten American's national security" maintained by the United States Treasury Department's Office of Foreign Assets Control ("OFAC"). *Id.* at 419–20. The plaintiff attempted to purchase a car from a dealership, but the dealership refused to sell him the vehicle after receiving a credit report from TransUnion that he was on OFAC's list. *Id.* at 420. It was stipulated by the parties that during the class period, TransUnion distributed similar reports to potential creditors concerning 1,853 of the 8,185 class members. *Id.* at 421.

The district court found that all 8,185 class members had standing to recover damages, and the Ninth Circuit affirmed. *Id.* at 422. The Supreme Court granted certiorari. *Id.* In evaluating the plaintiff's alleged injuries for standing purposes, the Supreme Court distinguished between the class members whose false OFAC designations had been sent to third parties and those whose names had not been disclosed. *Id.* at 432–33. As to the 1,853 class members whose

reports were disseminated, the Supreme Court had "no trouble" concluding that their injury, though intangible, was akin to the reputational harm of defamation—a harm traditionally recognized as providing a basis for lawsuits in American courts. *Id.* The Supreme Court did not "take further steps to evaluate whether those third parties *used* the information in ways that harmed the class members." *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 285 (2d Cir. 2023) (citing *TransUnion*, 594 U.S. at 433) (emphasis in original). As to the remaining class members whose credit reports were not shared with third parties, the Supreme Court concluded that they had not suffered a concrete injury because there is "no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury." *TransUnion*, 594 U.S. at 434 (internal quotation and citation omitted). The Supreme Court also rejected the remaining class members' efforts to establish standing to sue for damages based on a theory of a risk of future harm, reasoning that they had not demonstrated they "were independently harmed by their exposure to the risk itself—that is, that they suffered some other injury . . . from the mere risk that their credit reports would be provided to third-party businesses." *Id.* at 437. The Court, however, left open the possibility that "a plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm" but did not address the issue because the plaintiffs did not rely on this theory of harm to establish standing. *Id.* at 436 & n.7.

Plaintiff asks the Court to apply the principles articulated in *TransUnion* to find that he has standing based on his allegations of having suffered two primary types of injuries—(1) the intangible harm of having his PII published on the dark web, and (2) the imminent future harm of identity theft and fraud due to the data breach. The Fifth Circuit has not yet addressed Article III's injury requirement in the context of a data breach case, but other courts of appeals have

recently held that class action plaintiffs have standing to seek damages and injunctive relief in data breach cases based on similar allegations. *See Bohnak*, 79 F.4th at 285; *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 890 (11th Cir. 2023); *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 374–77 (1st Cir. 2023); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 157–58 (3d Cir. 2022). All of these cases were decided after and relied upon the reasoning of the Supreme Court's recent standing analysis in *TransUnion*. These cases are instructive and provide support for Plaintiff's arguments regarding both his alleged intangible injury and his alleged risk of future harm.

The Third Circuit's opinion in *Clemens v. ExecuPharm Inc.* focused on standing based on the alleged risk of future identity theft. The plaintiff in *Clemens* brought a class action against her former employer, a global pharmaceutical company, regarding a data breach at the company. 48 F.4th at 150. The plaintiff alleged that an identified hacking group stole the sensitive information of current and former employees, held the information for ransom, and then posted the data on the dark web where the information was made available for download. *Id.* The stolen data included names, Social Security numbers, birth dates, addresses, taxpayer IDs, banking information, credit card numbers, driver's licenses, tax forms, and passport numbers. *Id.* The complaint alleged that the plaintiff faced a risk of identity theft and fraud based on the data breach and the harm associated with the investment of time and money spent to mitigate the risk of that future injury. *Id.* at 151. The plaintiff alleged that, to prevent identity theft, she had reviewed her financial records and credit reports, transferred banking accounts to new financial institutions, and enrolled in credit monitoring. *Id.* The plaintiff also alleged that she had sustained therapy costs based on the emotional distress the breach caused her. *Id.* The district court dismissed the complaint for lack of jurisdiction, finding that an increased risk of identity

theft resulting from a security breach was insufficient to establish an Article III injury for purposes of standing. *Id.*

The Third Circuit reversed, applying *TransUnion* to hold that the substantial risk of identity theft or fraud can constitute a concrete injury where the plaintiff alleges both an imminent future injury and "additional, currently felt concrete harms." *Id.* at 155–56. In finding a concrete injury, the Third Circuit emphasized several factual components of the plaintiff's case that pushed the risk of future injury from merely hypothetical to imminent, relying on a framework for data breach cases developed by the Second Circuit in *McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295 (2d Cir. 2021). *Id.* at 153–54. In *McMorris*, the court identified three factors for courts to consider when asked to evaluate whether a plaintiff has alleged a concrete injury by alleging an increased risk of identity theft or fraud based on unauthorized data disclosure. 995 F.3d at 303. These factors include (1) whether the plaintiff's data was exposed as a result of a targeted attempt to obtain that data versus an inadvertent disclosure; (2) whether any portion of the dataset has already been misused, even if the plaintiff has not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive in nature, such as names and Social Security numbers (versus solely account numbers or banking information),[1] such that there is a high risk of identity theft or fraud. *Id.*

In *Clemens*, the Third Circuit applied the *McMorris* factors and found that the data breach was caused by a known ransomware group notorious for sophisticated hacking schemes and that the hackers had acted intentionally and already misused the data by encrypting it and

[1] *See also In re SuperValu, Inc.*, 870 F.3d 763, 770 (8th Cir. 2017) (noting that stolen credit card information "does not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers" and that this type of data "generally cannot be used alone to open unauthorized new accounts") (internal citation and quotation omitted).

posting it on the dark web after holding it for ransom. 48 F.4th at 156–57. Additionally, the type of data at issue could easily be used to perpetrate identity theft, as it included Social Security numbers, dates of birth, and full names of employees. *Id.* Finding the future risk of harm to be "sufficiently imminent and concrete," the Third Circuit also emphasized the fact that the lead plaintiff had alleged additional currently felt harms—emotional distress and related therapy costs and time and money involved in mitigating the fallout of the data breach. *Id.* at 156.

There are numerous parallels between the plaintiff's standing allegations in the *Clemens* case and Plaintiff's standing allegations here. Like the plaintiff in *Clemens*, Plaintiff alleges that the data breach at issue was caused by an intentional cyberattack by an identified "ransomware gang" known as "Akira." (Compl. [#1], at ¶ 25.) Additionally, the Complaint alleges that the gang had already misused the data by posting over 90 gigabytes of data on its "darknet leak site" and announced the intention to make 90 more gigabytes of data available in the near future. (*Id.*) There are also allegations that a group known as "KelvinSecurity Team" was already selling the stolen databases on a hacker forum. (*Id.* at ¶ 33.) As to the consideration of the type of data stolen, this case, like *Clemens*, involves the type of PII that could easily be used to perpetrate identity theft—names and Social Security numbers. (*Id.* at ¶ 22.) Based on the three *McMorris* factors, the risk of identity theft alleged by Plaintiff is not merely conjectural or speculative; there are concrete identifiable risks of imminent future harm to Plaintiff and the class members based on the posting of their PII on the dark web in hopes of selling the data for future gain. Finally, like the plaintiff in *Clemens*, Plaintiff alleges that he has already undertaken various steps to attempt to mitigate future harm. Plaintiff alleges that Defendant's letter informing its employees and clients of the breach directed those whose PII was stolen in the cyberattack to

review account statements, monitor credit reports, contact the three major credit reporting bureaus for copies of credit reports, and contact consumer reporting bureaus to take steps to protect the PII from identity theft, and that, as directed, Plaintiff has spent significant time and effort monitoring his accounts and enrolling in credit monitoring services. (*Id.* at ¶¶ 27, 48.)

The Third Circuit's decision in *Clemens* is not an outlier in its analysis of the alleged injury of the risk of future identity theft. The First, Second, and Eleventh Circuits have also found class plaintiffs to have alleged a concrete injury based on the risk of future identity theft and fraud based on even thinner allegations. In *Bohnak v. Marsh & McLennan Cos.*, the Second Circuit concluded that the plaintiff had alleged a concrete risk of imminent future harm where the class action complaint described a targeted and intentional data breach against the plaintiff's former employer, resulting in unauthorized access to employees' names and Social Security numbers, even though there were no allegations that the data had already been misused by the hackers. 79 F.4th at 289. Even though the plaintiff in *Bohnak* had not pleaded facts relevant to all three of the *McMorris* factors, the court found that "allegations of a targeted hack that exposed [her] name and SSN to an unauthorized actor are sufficient to suggest a substantial likelihood of future harm, satisfying the 'actual or imminent harm' component of an injury in fact." *Id.* The Second Circuit went on to conclude that the plaintiff had alleged additional injury—the costs incurred mitigating the consequences of the data breach—and that Plaintiff had standing to bring her claims for damages. *Id.* at 286.

Similarly, in *Webb*, the First Circuit concluded that the two lead plaintiffs in a data breach class action both had standing to pursue damages based on the plausible allegation of a "concrete injury in fact based on the material risk of future misuse" of PII and "a concrete harm caused by exposure to this risk." 72 F.4th at 374. Yet only one of the plaintiffs had experienced

actual identity theft through the filing of a fraudulent tax return. *Id.* at 370. The second plaintiff did not allege any known misuse of his data, and there were no allegations regarding the actual identity of the hacker or regarding the sale or posting of the stolen data on the dark web. *See id.* The First Circuit nonetheless concluded that future harm was imminent in light of the fact that the PII had been "deliberately taken by thieves intending to use the information to their financial advantage" through a "targeted attack rather than inadvertently"; that one of the employees had already experienced the misuse of the stolen data; and that the nature of the PII stolen (names and Social Security numbers) was particularly susceptible to misuse through identity theft. *Id.* at 375 (citing *McMorris*, 72 F.4th at 303).

The Eleventh Circuit similarly found a substantial risk of future injury even where the PII stolen was only financial information, rather than names and Social Security numbers at issue in the other circuit court cases and the case currently before the Court. *Green-Cooper*, 73 F.4th at 890. In *Green-Cooper*, the class action complaint alleged that hackers had targeted Chili's restaurant systems and stolen customer card data and personally identifiable information and then posted it on Joker Stash, an online marketplace for stolen payment data. *Id.* at 886–87. Two of the three named plaintiffs alleged that they had experienced unauthorized charges on the card they had used at Chili's; the third plaintiff canceled the card before ever experiencing fraudulent charges. *Id.* at 887. The Eleventh Circuit nonetheless held that all three named plaintiffs had adequately alleged a concrete injury sufficient for Article III standing to seek damages because they alleged their credit card and personal information was "exposed for theft and sale on the dark web" and there was a substantial risk of future injury through the misuse of the personal information associated with the hacked credit cards. *Id.* at 889–90.

Defendant argues, unconvincingly, that Plaintiff's asserted injuries are too speculative to constitute concrete harm, relying primarily on two 2015 district court cases from within the Fifth Circuit. *See Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015); *Green v. eBay Inc.*, Civil Action No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015). Not only do these cases predate *TransUnion* (which significantly diminishes their persuasive value), but they also were issued prior to the articulation of the *McMorris* framework and involved significant factual distinctions from the data breach allegations in this case.

In *Green*, in finding the alleged injuries to be too speculative to confer standing to pursue damages, the Louisiana district court emphasized that the class action complaint in that case did not contain any allegations that "any of the information accessed was actually misused or that there has even been an attempt to use it." 2015 WL 2066531, at *4. In contrast, here Plaintiff alleges the actual sale of the PII at issue on the dark web by known hacker entities. Additionally, in *Green* the court also emphasized that there was no evidence that "any financial information or Social Security numbers were accessed during the Data Breach," the precise opposite of the allegations here. *Id.*

The holding in *Peters* is also inapposite for several reasons. In *Peters*, the district court concluded that the alleged injuries suffered by the plaintiff as a result of the data breach—attempted charges to her credit card, attempted access to her Amazon.com account, spam email, and telephone solicitations—failed to confer standing because, according to the court, these injuries were not redressable through the suit because the plaintiff had not alleged any quantifiable damage or loss. 74 F. Supp. 3d at 857. Here, in challenging standing, Defendant is not arguing lack of redressability. As to the future risk of identity theft, the Texas district court summarily dismissed the injury as too speculative based on vague allegations of an increased risk

of future identity theft without the supporting allegations regarding the nature of the attack and the actual misuse of the data on a large scale by ransomware gangs pleaded here. *See id.*

In contrast, the detailed allegations in the Class Action Complaint currently before the Court fit squarely into both the *McMorris* framework for evaluating the imminence of future harm from a data breach and the Supreme Court's recognition of a substantial and imminent risk of future harm as a concrete Article III injury where there are allegations of a separate concrete harm caused by the "exposure to the risk itself." *TransUnion*, 594 U.S. at 437. In summary, Plaintiff has pleaded a concrete Article III injury to support his claim for damages based on the actual and imminent risk of future identity theft and the separate harm caused by that risk, namely the expenditure of time and money enrolling in credit monitoring services.[2]

That leaves the question of whether Plaintiff's Complaint also alleges another type of concrete injury recognized by the Supreme Court in *TransUnion*—an intangible harm bearing a close relationship to a harm traditionally recognized by the courts, such as the reputational harm at issue in the Supreme Court's case. Plaintiff asks the Court to also find that the publication of PII on the dark web is itself a concrete injury sufficient to confer standing to pursue damages in a data breach case. The Eleventh Circuit endorsed this reasoning in *Green-Cooper*, as did the

[2] The undersigned notes that prior to *TransUnion*, the Supreme Court rejected a theory of standing based on the cost of mitigation measures taken to protect a plaintiff's communications from being the subject of unauthorized surveillance. *Clapper*, 568 U.S. at 401. The holding in *Clapper* does not foreclose the Court's consideration of the mitigation measures allegedly taken by Plaintiff in this case. With respect to costs incurred to mitigate a future risk of harm, the thrust of the *Clapper* decision was that a plaintiff "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." *Id.* at 402. The Supreme Court in *Clapper* first concluded that the plaintiffs had failed to allege an imminent and "certainly impending" future injury. *Id.* at 401–02. Here, Plaintiff has pleaded an imminent and concrete risk of future harm and therefore may also rely on related currently felt harms to establish standing to pursue damages. Also, it is notable that here, Plaintiff cannot be accused of manufacturing standing given the allegation that Plaintiff was directed to take mitigation measures by Defendant.

Second Circuit in *Bohnak*. The Eleventh Circuit concluded that having one's credit card data and personal information "floating around on the dark web" was itself a present intangible injury and established standing to sue for damages. *Green-Coooper*, 73 F.4th at 890. The Second Circuit similarly concluded that the unauthorized access to a person's name and Social Security number was similar to the harm suffered as a result of the tort of public disclosure of private facts—a harm traditionally recognized by the courts—and was also analogous to the publication of misleading information to third parties at issue in *TransUnion*. *Bohnak*, 79 F.4th at 285.

The same conclusion is supported by Plaintiff's allegations in this case. The Supreme Court's recognition of the intangible harm caused by the distribution of inaccurate credit information to third parties in *TransUnion* reasonably can be extended to the context of the largescale publication of stolen PII on the dark web—a marketplace for selling personal information to actors with nefarious intent—and the actual sale of that material. As the Second Circuit noted, this type of alleged harm is analogous to the harm associated with the common-law analog of public disclosure of private facts. *See TransUnion*, 594 U.S. at 436. Accordingly, in addition to pleading a concrete and imminent risk of future identity theft, Plaintiff has pleaded the current intangible injury associated with the publication and sale of his PII on the dark web.

Based on the foregoing, the District Court should deny Defendant's motion to dismiss for lack of standing and conclude that Plaintiff has sufficiently alleged both the future risk of imminent identity theft and the intangible harm associated with the posting of his PII on the dark web. Given that the undersigned has found two types of injuries, each sufficient to confer standing to pursue damages on its own, the Court need not address Plaintiff's other theories of standing based on damage to Plaintiff's property interest in his PII, the increase in scam messages and calls, or a violation of Plaintiff's implied contractual rights.

IIII. Failure to State a Claim

Defendant also asks the Court to dismiss several of Plaintiff's claims for failure to state a claim pursuant to Rule 12(b)(6). For the reasons that follow, the Court should grant Defendant's motion to dismiss as to Plaintiff's breach-of-fiduciary-duty claim and his invasion-of-privacy claim, but his other claims should survive Defendant's motion.

A. Legal Standard

To survive a motion to dismiss under Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "Although a complaint "does not need detailed factual allegations," the "allegations must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. The allegations pleaded must show "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678. In short, a claim should not be dismissed unless the court determines that it is beyond doubt that the plaintiff cannot prove a plausible set of facts that support the claim and would justify relief. *See Twombly*, 550 U.S. at 570. In reviewing a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a court "accepts all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff." *Martin K. Eby Const. Co. v. Dallas Area Rapid Transit*, 369 F.3d 464, 467 (5th Cir. 2004) (internal quotation omitted). However, a court need not credit conclusory allegations or allegations that merely restate the legal elements of a claim. *Chhim v. Univ. of Tex. at Austin*, 836 F.3d 467, 469 (5th Cir. 2016) (citing *Iqbal*, 556 U.S. at 678).

B. Analysis

Defendant argues that Plaintiff's claims for breach of implied contract, breach of fiduciary duty, invasion of privacy, and unjust enrichment all fail as a matter of law. Defendant does not seek dismissal of Plaintiff's negligence and negligence *per se* claims. The Court should dismiss Plaintiff's breach-of-fiduciary-duty and invasion-of-privacy claims but deny Defendant's motion as to the claims for breach of implied contract and unjust enrichment.

i. Breach of Implied Contract

Plaintiff's Complaint pleads a cause of action for breach of implied contract on behalf of himself and the proposed class. (Compl. [#1], at ¶¶ 121–37.) The elements for a breach-of-an-implied-contract claim in Texas are: (1) the existence of a valid implied contract; (2) performance or tendered performance by the plaintiff; (3) breach of the implied contract by the defendant; and (4) damages resulting from the breach. *USAA Tex. Lloyds Co. v. Menchaca*, 545 S.W.3d 479, 501 n.21 (Tex. 2018) (listing elements for claim of breach of contract); *Plotkin v. Joekel*, 304 S.W.3d 455, 476 (Tex. App.—Houston [1st Dist.] 2009, pet. denied) (noting that elements of breach of contract are identical whether contract is express or implied). To adequately plead the existence of a valid implied contract, a plaintiff must plead facts that support the same elements as for express contracts: (1) an offer; (2) an acceptance; (3) mutual assent or a meeting of the minds; (4) each party's consent to the terms; and (5) execution and delivery of the contract with the intent that it be mutual and binding. *DeClaire v. G & B McIntosh Family Ltd. P'ship,*, 260 S.W.3d 34, 44 (Tex. App.—Houston [1st Dist.] 2008, no pet.). Defendant argues Plaintiff has failed to plead facts in support of the first element of his breach-of-implied-contract claim because he has not pleaded facts that would demonstrate the existence of a valid implied contract regarding a promise to safeguard Plaintiff's PII.

Specifically, Defendant argues that there was no meeting of the minds between the parties to support the finding of an implied contract.

The Court should reject Defendant's argument and find that Plaintiff's Complaint pleads a cause of action for breach of implied contract and allow this claim to proceed past the pleading stage. The basis of Plaintiff's implied contract claim is that he, like other employees of Defendant/putative class members, was required to provide his PII to Defendant as a condition of employment (and that the putative class members who were clients of Defendant were also required to do so as a condition of receiving Defendant's services). (Compl. [#1], at ¶ 122.) Plaintiff alleges that there was an implied promise by Defendant to protect and not disclose the PII to unauthorized persons, as evidenced by Defendant's Privacy Policy. (*Id.* at ¶¶ 125–127.)

According to the Complaint, Defendant's Privacy Policy "governs [Defendant's] data collection, processing, and usage practices" and promises to use the PII "only in compliance with this Privacy Policy." (*Id.* at ¶ 127.) The Privacy Policy assures employees and clients that Defendant "will never sell" PII to any third party; that Defendant "adheres to the Privacy Shield Principles" of the U.S. Department of Commerce; that Defendant "has a consistent level of data protection and security" across the organization; that Defendant's breach procedures ensure the identification, assessment, investigation, and reporting of "any personal data breach within 72 hours of becoming aware of the breach"; and that Defendant uses "a variety of security technologies and procedures to help protect . . . personal data from unauthorized access, use or disclosure" and has "robust information security policies and procedures in place to protect personal information from unauthorized access." (*Id.* at ¶ 19.) Plaintiff asserts that these promises gave rise to an implied contract and that Defendant breached the contract by failing to safeguard his information; failing to notify him promptly of the intrusion into its computer

systems; failing to comply with industry standards; failing to comply with the legal obligations incorporated into the agreements; and failing to ensure confidentiality and integrity of PII. (*Id.* at ¶ 133.)

Defendant's motion does not cite any case applying Texas law addressing a breach of implied contract claim in the context of a data breach case. And the undersigned found none. However, the undersigned's independent research revealed that many districts courts have denied motions to dismiss claims of breach of implied contract where the movant argues the plaintiff's pleadings do not plead facts to support that a valid implied contract exists, but the alleged implied contract arises in the employer-employee context, and there are documents outside of the employment contract itself addressing the employer's policies as to data retention and protection. *See Archey v. Osmose Utilities Servs., Inc.*, No. 20-CV-05247, 2022 WL 3543469, at *4 (N.D. Ill. Aug. 18, 2022) (noting that courts "that have found an implied contract in the employee-employer data breach context have done so when the plaintiffs were able to point to some document, expression, or action of the employer which indicated an intention to protect the employee's personal information"). And privacy policies like the one described in Plaintiff's Complaint have been recognized as a plausible basis for finding that a valid implied contract exists under various state laws across the country. *See In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 591 (N.D. Ill. 2022) (denying motion to dismiss a breach-of-implied-contract claim where the plaintiffs pleaded the existence of a privacy policy applying to personal information collected by the employer); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 486 (D. Md. 2020) (denying motion to dismiss under Oregon law on basis that Marriott and Starwood's privacy statements concerning their collection and use of personal information of customers could plausibly form basis of breach-of-implied-contract

claim); *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 801 (W.D. Wis. 2019) (finding it was reasonable to infer that the parties intended to incorporate the defendant's privacy policy regarding the protection of PII into their contract for health services); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 750 (S.D.N.Y. 2017) (denying motion to dismiss breach-of-implied-contract claim where the employer's privacy policy and security-practices manual stated that it "maintains robust procedures designed to carefully protect the PII with which it [is] entrusted"). Such policies plausibly support "a finding of an implicit promise to protect employees' personal information in exchange for their employment" or in exchange for their business. *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d at 591; *see also McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019) (denying motion to dismiss breach-of-implied-contract claim where employee alleged that employer implicitly agreed to safeguard the employee's PII by requiring employees to provide said information as a condition of employment).

In contrast, courts have dismissed breach-of-implied-contract claims where a plaintiff's pleadings do not identify any company-specific documents or policies from which one could infer an implied contractual duty to protect the plaintiff's personal information. *See, e.g.*, *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1221 (11th Cir. 2023) (affirming dismissal of a breach-of-implied-contract claim under Georgia law where plaintiff only made "bare assertion" that defendants agreed to safeguard his PII without any allegations that defendants agreed to be bound by any data retention or protection policy); *Longenecker-Wells v. Benecard Servs. Inc.*, 658 Fed. App'x 659, 662–63 (3d Cir. 2016) (affirming dismissal of a breach-of-implied-implied contract claim where plaintiffs failed to plead any facts beyond the employment relationship upon which a contractual promise to safeguard PII from third-party hackers could be inferred);

Antman v. Uber Techs., Inc., Case No. 15-cv-01175-LB, 2018 WL 2151231, at *12 (N.D. Cal. May 10, 2018) (granting motion to dismiss claim of breach of implied contract where plaintiffs failed to plead any facts about an implied contract regarding security of private information). Consistent with the well-reasoned decisions described above, the undersigned concludes that Plaintiff has sufficiently pleaded facts that, if ultimately proven, would demonstrate that an implied contract exists.[3]

ii. Breach of Fiduciary Duty

Plaintiff's claim of breach of fiduciary duty alleges that Defendant had a fiduciary duty to act for the benefit of Plaintiff and the putative class members in securing their PII and that Defendant breached that duty by failing to sufficiently protect their PII and failing to diligently discover, investigate, and give notice of the data breach. (Compl. [#1], at ¶¶ 138–44.) The elements of a breach-of-fiduciary-duty claim are: (1) a fiduciary relationship between the plaintiff and defendant; (2) the breach of that duty; and (3) an injury to the plaintiff or benefit to the defendant. *Jones v. Blume*, 196 S.W.3d 440, 447 (Tex. App.—Dallas 2006, pet. denied). Defendant argues Plaintiff fails to plead facts to support the existence of a fiduciary duty between the parties because Texas law forecloses such a duty in the context of an employer-employee relationship. The undersigned agrees.

It is well settled that "[i]n Texas, employers generally do not owe fiduciary duties to their employees." *Meadows v. Hartford Life Ins. Co.*, 492 F.3d 634, 639 (5th Cir. 2007) (citing *Beverick v. Koch Power, Inc.*, 186 S.W.3d 145, 153 (Tex. App.—Houston [1st Dist.] 2005, reh'g

[3] The undersigned notes that Plaintiff refers to a breach of the duty of good faith and fair dealing in context of his allegations supporting his breach-of-implied-contract claim. Defendant makes several arguments regarding the duty of good faith and fair dealing in its motion to dismiss. The undersigned does not construe Plaintiff's Complaint as pleading a separate claim based on the covenant of good faith and fair dealing and therefore has not and need not address these arguments.

overruled (Mar. 13, 2006), review denied (Jun. 2, 2006)) ("Texas does not recognize a fiduciary duty . . . owed by an employer to an employee."). Numerous federal courts have dismissed fiduciary-duty claims in the employment context on this basis. *See, e.g.*, *Arizmendi v. ORC Indus.*, Civ. A. No. B-06-125, 2007 WL 1231464, at *1 (S.D. Tex. Apr. 26, 2007); *Garcia v. Communities in Schs. of Brazoria Cnty, Inc.*, Civ. A. No. H-18-4558, 2019 WL 2420079, at *11 (S.D. Tex. June 10, 2019).

Plaintiff argues that it is premature to dismiss the breach-of-fiduciary-duty claim because there was a "special relationship" between Plaintiff and Defendant giving rise to a fiduciary duty to safeguard the PII. Yet Plaintiff has not directed the Court to any case finding that an employer has a fiduciary duty to its employees. A special relationship of trust and confidence may, however, impose an informal fiduciary duty in the context of a business transaction. *See Transport Ins. Co. v. Faircloth*, 898 S.W.2d 269, 280 (Tex. 1995). But Plaintiff was not in a business relationship with Defendant and has not pleaded any such special relationship here. Accordingly, the Court should grant Defendant's motion to dismiss as to Plaintiff's breach of fiduciary duty claim.

iii. Invasion of Privacy

Defendant also seeks dismissal of Plaintiff's claim of invasion of privacy. There are two elements to this tort under Texas law: "(1) an intentional intrusion, physically or otherwise upon another's solitude, seclusion or private affairs or concerns" that "(2) would be highly offensive to a reasonable person." *Amin v. United Parcel Serv., Inc.*, 66 F.4th 568, 576 (5th Cir. 2023) (quoting *Valenzuela v. Aquino*, 853 S.W.2d 512, 513 (Tex. 1993)). Also, "Texas courts have held that intrusion upon private affairs typically requires either a trespass or an attempt to discover or perceive private information." *Id.* at 577. Defendant argues that, although hacking

into a private computer could give rise to a privacy claim, *see Hovanec v. Miller*, Civ. A. No. SA-17-CV-766-XR, 2018 WL 1221486, at *10 (W.D. Tex. Mar. 7, 2018), that claim may only be asserted against the hackers themselves—not Defendant. Defendant contends that Plaintiff has not alleged a plausible theory of invasion of privacy based on any intrusion *by Defendant* upon Plaintiff's private affairs, as Plaintiff does not allege that Defendant took any action directed towards Plaintiff that led to the data breach.

Plaintiff responds that in Texas an invasion-of-privacy claim can be based on a negligent or an intentional act, and that Defendant negligently stored Plaintiff's data, making it vulnerable to a data breach. There is a split among Texas courts of appeals on whether to recognize a cause of action for negligent invasion of privacy. *Compare Doe v. Mobile Video Tapes, Inc.*, 43 S.W.3d 40, 54 (Tex. App.—Corpus Christi-Edinburg 2001, reh'g overruled) ("Although some courts in Texas recognize negligent invasion of privacy, we decline to adopt a negligent invasion of privacy cause of action."); *Childers v. A.S.*, 909 S.W.2d 282, 291 (Tex. App.—Fort Worth 1995, no writ) (declining to adopt a negligent-invasion-of-privacy claim) *with Boyles v. Kerr*, 806 S.W.2d 255, 259 (Tex. App.—Texarkana 1991), *rev'd on other grounds*, 855 S.W.2d 593 (Tex. 1993) (op. on reh'g) ("[T]he basis for liability in a privacy action may rest upon a negligent, as well as an intentional, invasion."); *C.T.W. v. B.C.G.*, 809 S.W.2d 788, 796 (Tex. App.—Beaumont 1991, no writ) ("An intrusion or violation of personal privacy can be brought about negligently . . . ."). The reasoning of those courts rejecting such a cause of action is more persuasive and better predicts how the Texas Supreme Court would likely resolve the split in authority. Thus, the District Court should dismiss this claim.

In applying Texas law, this Court must first look to the decisions of the Texas Supreme Court. *Ironshore Europe DAC v. Schiff Hardin, L.L.P.*, 912 F.3d 759, 764 (5th Cir. 2019). If the

Texas Supreme Court has not ruled on an issue, this Court must make an *Erie* guess, predicting what the Texas Supreme Court would do if faced with the same facts. *Id.* Intermediate state court decisions are typically "the strongest indicator of what a state supreme court would do, absent a compelling reason to believe that the state supreme court would reject the lower courts' reasoning." *Hux v. S. Methodist Univ.*, 819 F.3d 776, 780 (5th Cir. 2016).

The Texas Supreme Court defines the invasion of privacy as an intentional tort. *Billings v. Atkinson*, 489 S.W.2d 858, 861 (Tex. 1973) (describing the invasion of privacy as a "willful tort which constitutes legal injury"). The Texas Supreme Court is likely to reject a negligent theory of invasion of privacy if faced with such a claim. In *Boyles*, one of the two cases cited by Plaintiff recognizing a negligent-invasion-of-privacy claim, the court of appeals had endorsed both a claim of negligent invasion of privacy and negligent infliction of emotional distress. 806 S.W.2d at 259. On appeal from that decision, the Texas Supreme Court reversed the court of appeals as to the claim of negligent infliction of emotional distress, reasoning that infliction of emotional distress is an intentional tort. *Boyles v. Kerr*, 855 S.W.2d 593, 595–97 (Tex. 1993). In doing so, the Texas Supreme Court overruled its prior precedent in *St. Elizabeth Hosp. v. Garrard*, 730 S.W.2d 649 (Tex. 1987), which had recognized a negligent-infliction-of-emotional-distress claim. *Id.* The Supreme Court did not address the negligent-invasion-of-privacy claim because the plaintiff in *Boyles* abandoned the claim before the Supreme Court's decision. *Id.* at 601. Had the claim still been a part of the case, the Texas Supreme Court would have been likely to reject the claim based on the same reasoning.

The only other case relied upon by Plaintiff, *C.T.W.* (cited *supra*), was decided prior to *Boyles* and relied upon *Garrard* and the negligent theory for an intentional-infliction-of-distress claim in extending the lesser intent requirement to the invasion-of-privacy context. 809 S.W.2d

at 796. In light of the overruling of *Garrard* by the Texas Supreme Court and its holding that Texas no longer recognizes a separate cause of action for negligent infliction of emotional distress, this Court should decline to follow the outdated courts of appeals decisions recognizing a negligent-invasion-of-privacy claim.

Additionally, several federal district court decisions have rejected Plaintiff's theory and dismissed invasion-of-privacy claims based on a theory of negligence or vicarious liability as unavailable under Texas law. *See, e.g.*, *Jackson v. Methodist Hosps. of Dallas*, No. 3:05-CV-1345-N, 2006 WL 8437071, at *1 (N.D. Tex. July 19, 2006) (emphasizing that invasion of privacy is an intentional tort and dismissing negligent invasion of privacy claim); *Aguinaga v. Sanmina Corp.*, No. 3:97-CV-1026-G, 1998 WL 241260, *4 (N.D. Tex. 1998) (emphasizing that invasion of privacy is an intentional tort and dismissing invasion-of-privacy claim based on a theory of vicarious liability). In summary, the Court should grant Defendant's motion to dismiss as to Plaintiff's invasion-of-privacy claim.

iv. Unjust Enrichment

The last cause of action challenged by Defendant is Plaintiff's unjust-enrichment claim. Defendant's primary argument for the dismissal of this claim is that it is not an independent cause of action but rather a theory of recovery dependent on another viable cause of action. Defendant argues that because all of Plaintiff's claims fail for lack of standing or as a matter of law, this cause of action must be dismissed as well. The Court should reject this argument as a basis for dismissal of Plaintiff's unjust-enrichment allegations.

First, although there is some confusion among the courts as to whether unjust enrichment is an independent cause of action or merely a quasi-contractual theory of recovery, *see Perales v. Bank of Am., N.A.*, No. CIV.A. H-14-1791, 2014 WL 3907793, at *3 (S.D. Tex. Aug. 11, 2014)

(surveying Texas law), the Texas Supreme Court has repeatedly recognized and affirmed claims of unjust enrichment. *See Ye v. Zhang*, No. 4:18-CV-4729, 2021 WL 5862093, at *2 (S.D. Tex. June 8, 2021) (citing *Trial v. Dragon*, 593 S.W.3d 313, 323 n.6 (Tex. 2019) (referring to unjust enrichment and money had and received as distinct claims); *Fortune Prod. Co. v. Conoco, Inc.*, 52 S.W.3d 683, 683 (Tex. 2000) (discussing unjust enrichment as a "claim" based on quasi-contract), *HECI Exploration Co. v. Neel*, 982 S.W.2d 881, 891 (Tex. 1998) (recognizing unjust-enrichment claim). Moreover, the undersigned has concluded that most of Plaintiff's claims should survive Defendant's motion to dismiss. Plaintiff pleads unjust enrichment "in the alternative to his breach of contract claim." (Compl. [#1], at ¶ 161.) Plaintiff is permitted to plead alternative theories of recovery. Fed. R. Civ. P. 8(a)(3). Accordingly, the Court should deny Defendant's motion to dismiss on this basis.

Defendant also argues that Plaintiff has failed to plead the elements of this cause of action. Regardless of whether unjust enrichment is properly characterized as a cause of action or a theory of recovery, the elements of proof are clear. "To recover under unjust enrichment, a claimant must prove: (1) that valuable services were rendered or materials furnished; (2) for the person sought to be charged; (3) which services and materials were accepted by the person sought to be charged, used, and enjoyed by that person; and (4) under such circumstances as reasonably notified the person sought to be charged that the plaintiff in performing such services was expecting to be paid by the person sought to be charged." *Reveille Trucking, Inc. v. Lear Corp.*, No. 4:14-CV-511, 2017 WL 661521, at *13 (S.D. Tex. Feb. 17, 2017). "Under Texas law an unjust enrichment claim requires showing that one party 'has obtained a benefit from another by fraud, duress, or the taking of an undue advantage.'" *Digital Drilling Data Sys., L.L.C. v. Petrolink Servs., Inc.*, 965 F.3d 365, 379–80 (5th Cir. 2020) (quoting *Heldenfels Bros., Inc. v.*

City of Corpus Christi, 832 S.W.2d 39, 41 (Tex. 1992)). Defendant argues that Plaintiff has failed to adequately allege that Defendant obtained a benefit from Plaintiff by fraud, duress, or taking of an undue advantage. The undersigned disagrees.

Plaintiff pleads that Defendant is liable for unjust enrichment because it benefited from the provision of PII (which was required to collect payment from clients or to facilitate the employment of employees) and therefore facilitated its ability to provide its business consulting services worldwide. (Compl. [#1], at ¶¶ 162–63.) Plaintiff further alleges that rather than providing adequate security measures, it "enriched itself by saving the costs they reasonably should have expended" on such measures and avoided its data-security obligations at Plaintiff's and the class members' expense. (*Id.* at ¶¶ 165–66.)

Defendant has not provided the Court with any authority supporting its argument that Plaintiff cannot plead undue advantage by asserting that Defendant unjustly benefited from shirking its data-security obligations by skimping on security measures and leaving Plaintiff to suffer the consequences. The Court should allow this claim and/or theory of recovery to proceed past the pleading stage and deny Defendant's motion to dismiss on this basis.

IV. Conclusion and Recommendation

Having considered the motion, response, and reply, and the governing law, the undersigned recommends that Defendant Frost & Sullivan, Inc.'s Rule 12(b)(1) Motion to Dismiss for Lack of Subject Matter Jurisdiction and Rule 12(b)(6) Motion to Dismiss for Failure to State a Claim [#7] be **granted in part** as to Plaintiff's breach-of-fiduciary-duty and invasion-of-privacy claims. In all other respects, the motion should be **denied**. Plaintiff has standing to pursue his claims for damages and injunctive relief, and his claims of negligence, negligence *per se*, breach of implied contract, and unjust enrichment shall survive Defendant's motion.

V. Instructions for Service and Notice of Right to Object/Appeal

The United States District Clerk shall serve a copy of this report and recommendation on all parties by either (1) electronic transmittal to all parties represented by attorneys registered as a "filing user" with the clerk of court, or (2) by mailing a copy to those not registered by certified mail, return receipt requested. Written objections to this report and recommendation must be filed **within fourteen (14) days** after being served with a copy of same, unless this time period is modified by the district court. 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b). The party shall file the objections with the Clerk of Court and serve the objections on all other parties. A party filing objections must specifically identify those findings, conclusions or recommendations to which objections are being made and the basis for such objections; the district court need not consider frivolous, conclusive or general objections. A party's failure to file written objections to the proposed findings, conclusions and recommendations contained in this report shall bar the party from a *de novo* determination by the district court. *Thomas v. Arn*, 474 U.S. 140, 149–52 (1985); *Acuña v. Brown & Root, Inc.*, 200 F.3d 335, 340 (5th Cir. 2000). Additionally, failure to file timely written objections to the proposed findings, conclusions and recommendations contained in this report and recommendation shall bar the aggrieved party, except upon grounds of plain error, from attacking on appeal the un-objected-to proposed factual findings and legal conclusions accepted by the district court. *Douglass v. United Servs. Auto. Ass'n*, 79 F.3d 1415,

1428–29 (5th Cir. 1996) (en banc), *superseded by statute on other grounds*, 28 U.S.C. § 636(b)(1).

SIGNED this 16th day of August, 2024.

ELIZABETH S. ("BETSY") CHESTNEY
UNITED STATES MAGISTRATE JUDGE